Journal de Théorie des Nombres
de Bordeaux **13** (2001), 651–658

Multiplicative functions and k-automatic sequences

par Soroosh YAZDANI

Résumé. Une suite est dite k-automatique si son $n^{\rm e}$ terme peut être engendré par une machine à états finis lisant en entrée le développement de n en base k. Nous prouvons que, pour de nombreuses fonctions multiplicatives f, la suite $(f(n) \bmod v)_{n\geq 1}$ n'est pas k-automatique. C'est en particulier le cas pour les fonctions multiplicatives $\tau_m(n)$, $\sigma_m(n)$, $\mu(n)$ et $\phi(n)$.

Abstract. A sequence is called k-automatic if the n'th term in the sequence can be generated by a finite state machine, reading n in base k as input. We show that for many multiplicative functions, the sequence $(f(n) \bmod v)_{n\geq 1}$ is not k-automatic. Among these multiplicative functions are $\tau_m(n)$, $\sigma_m(n)$, $\mu(n)$, and $\phi(n)$.

We call a function $f : \mathbb{N}\setminus\{0\} \to \mathbb{C}$ multiplicative, if for all $m, n \in \mathbb{N}\setminus\{0\}$, m and n coprime, we have $f(mn) = f(m)f(n)$. As usual let $\tau(n)$, $\sigma(n)$, $\phi(n)$, $\mu(n)$ represent the number of divisors of n, sum of the divisors of n, number of numbers less than or equal to n and prime to n, and the Möbius function respectively. We know that $\tau(n)$, $\sigma(n)$, $\phi(n)$, and $\mu(n)$ are multiplicative. Also let $\tau_m(n)$ be number of elements in $\big\{(a_1, a_2, \cdots, a_m) \mid a_1a_2\cdots a_m = n \text{ and } a_1, a_2, \ldots, a_m \in \mathbb{N}\setminus\{0\}\big\}$. Then we have

$$\tau_m(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}) = \prod_{i=1}^{t}\binom{m+\alpha_i-1}{m-1}, \tag{1}$$

where p_i's are distinct primes (see for example [9, p. 72]). Furthermore let

$$\sigma_m(n) = \sum_{k\mid n} k^m.$$

Recall that $\sigma_m(n)$ is multiplicative for all integers m. Note that $\sigma_1(n) = \sigma(n)$, and $\tau_2(n) = \tau(n)$.

Manuscrit reçu le 5 octobre 1999.

Given $k \geq 2$, we say a sequence $\mathbf{T} = (t(n))_{n\geq 1}$ is k-automatic if and only if

$$\mathbf{T}^{(k)} = \left\{ \mathbf{T}^{(k)}_{l,r} \mid l \geq 0 \text{ and } 0 \leq r < k^l \right\}$$

is finite, where $\mathbf{T}^{(k)}_{l,r} = (t(k^l n + r))_{n\geq 1}$. The set $\mathbf{T}^{(k)}$ is called the k-kernel of $\mathbf{T}$. We say a set $S \subset \mathbb{N} \setminus \{0\}$ is k-automatic if the sequence $(\chi_S(n))_{n\geq 1}$ is k-automatic, where

$$\chi_S(n) = \begin{cases} 1 & \text{if } n \in S, \\ 0 & \text{otherwise.} \end{cases}$$

If $t : \mathbb{N} \setminus \{0\} \to X$ for some set X, and if there is a mapping $\Phi : X \to Y$, then we can extend Φ to sequences in X with $\Phi(\mathbf{T}) = (\Phi(t(n))_{n\geq 1})$. Note that

$$\Phi : \mathbf{T}^{(k)} \to (\Phi(\mathbf{T}))^{(k)}$$

is an onto mapping. Specifically note that the cardinality of $\mathbf{T}^{(k)}$ is greater than or equal to the cardinality of $\Phi(\mathbf{T})^{(k)}$, and hence if $\mathbf{T}$ is k-automatic, then so is $\Phi(\mathbf{T})$. Therefore we have the following,

Lemma 1. *Let $(f(n))_{n\geq 1}$ be a sequence of integers. If there exist integers $v, k \geq 2$ such that $(f(n) \bmod v)_{n\geq 1}$ is k-automatic, then for all $q|v$ we have that the sequence $(f(n) \bmod q)_{n\geq 1}$ is also k-automatic.*

The term k-automatic is used because one can compute $t(n)$ by feeding the base k representation of n as an input to a finite state machine [5]. In [3], see also [4], it is shown that given prime p and a sequence $(t(n))_{n\geq 1}$ with values in $\mathbb{F}_p$, then

$$F(X) = \sum_{n\geq 0} t(n) X^n \in \mathbb{F}_p[[X]]$$

is algebraic over $\mathbb{F}_p(X)$ if and only if $(t(n))_{n\geq 1}$ is p-automatic.

Now we proceed to prove the first theorem in this paper, whose proof is a variation of a proof suggested by J. Shallit.

Theorem 2. *Let $v > 1$ be an integer and f a multiplicative function. Assume that for some integer $h \geq 1$ there exist infinitely many primes q_1 such that $f(q_1^h) \equiv 0 \pmod v$. Furthermore assume that there exist relatively prime integers b and c such that for all primes $q_2 \equiv c \pmod b$ we have $f(q_2) \not\equiv 0 \pmod v$. Then the sequence $F = (f(n) \bmod v)_{n\geq 1}$ is not k-automatic for any $k \geq 2$.*

Proof. Choose an arbitrary integer $k \geq 2$. Since $\gcd(b, c) = 1$, by Dirichlet's theorem there exists some integer m such that $bm + c > k$, and $bm + c$ is prime. Letting $a = bm + c$, we get $\gcd(a, bk) = 1$.

Now we will show that given $l, r_1, r_2 \in \mathbb{N} \setminus \{0\}$ such that $k^l > 2bk$, $0 \le r_1 \ne r_2 < k^l$, and $r_2 \equiv a \pmod{bk}$, there exists $n \in \mathbb{N} \setminus \{0\}$ such that $f(k^l n + r_1) \not\equiv f(k^l n + r_2) \pmod{v}$, hence $F^{(k)}_{l,r_1} \ne F^{(k)}_{l,r_2}$. This in turn means that the k-kernel of F is infinite, which means that F is not k-automatic.

Choose a prime $q_1 > k^l$ such that $f(q_1^h) \equiv 0 \pmod{v}$. Observe that $\gcd(bk^l, q_1^h) = 1$ since q_1 is prime and $q_1 > k^l > b$. Hence there exists an integer n_0 such that

$$n_0 b k^l + r_1 \equiv q_1^h \pmod{q_1^{h+1}}. \tag{2}$$

Furthermore observe that

$$\begin{aligned} n_0 b k^l + r_2 &\equiv r_2 \pmod{b} \\ &\equiv a \pmod{b}, \end{aligned}$$

for all n_0. Therefore for all $j \in \mathbb{N} \setminus \{0\}$, we have

$$q_1^h \parallel bk^l(n_0 + j q_1^{h+1} b) + r_1$$

and

$$bk^l(n_0 + j q_1^{h+1} b) + r_2 \equiv a \pmod{b}. \tag{3}$$

We need to show that for some j, $n_0 + j q_1^{h+1} b > 0$ and the left-hand side of Equation (3) is prime. To do so we will show that $\gcd(n_0 b k^l + r_2, k^l q_1^{h+1} b^2) = 1$, and apply Dirichlet's theorem.

Note that $r_2 \equiv a \pmod{k}$, and $\gcd(a, k) = 1$. Therefore

$$\gcd(k^l, n_0 b k^l + r_2) = \gcd(k^l, r_2) = 1.$$

Also $n_0 b k^l + r_2 \equiv a \pmod{b}$. Since $\gcd(a, b) = 1$, we get

$$\gcd(b, n_0 b k^l + r_2) = \gcd(b, r_2) = 1.$$

Finally from Equation (2) we have that $n_0 b k^l + r_2 \equiv q_1^h + r_2 - r_1 \pmod{q_1^{h+1}}$. We know that $r_1 \ne r_2$, and $0 \le r_1, r_2 < k^l < q_1$. Since q_1 is prime, we get that

$$\gcd(q_1, n_0 b k^l + r_2) = \gcd(q_1, r_2 - r_2) = 1.$$

Therefore $\gcd(n_0 b k^l + r_2, k^l q_1^{h+1} b^2) = 1$. Hence by Dirichlet's theorem, we can find an integer $j > |n_0|$ such that

$$\begin{aligned} k^l q_1^{h+1} b^2 j + n_0 b k^l + r_2 &\equiv a \pmod{b} \\ &\equiv c \pmod{b} \end{aligned}$$

is prime. By hypothesis, $f(k^l(q_1^{h+1} b^2 j + b n_0) + r_2) \bmod v \ne 0$.

On the other hand we have that by Equation (2)

$$q_1^h \parallel k^l(q_1^{h+1} b^2 j + b n_0) + r_1.$$

Since f is multiplicative, we have $f(k^l(q_1^{h+1} b^2 j + b n_0) + r_1) \bmod v = 0$. Letting $n = q_1^{h+1} b^2 j + b n_0$, we get $f(k^l n + r_1) \not\equiv f(k^l n + r_2) \pmod{v}$.

Therefore F is not k-automatic for any $k \geq 2$. $\square$

From this theorem we immediately get the following corollaries.

Corollary 3. *Given $m \geq 1$ and $v \geq 3$, the sequence $(\sigma_m(n) \bmod v)_{n\geq 1}$ is not k-automatic for any $k \geq 2$.*

Proof. Given an integer $v \geq 3$, there are infinitely many primes $q_1 \equiv 1 \pmod{v}$. Taking $h = v-1$ we get

$$\begin{aligned} \sigma(q_1^{v-1}) &\equiv \sum_{k \mid q_1^{v-1}} k^m \pmod{v} \\ &\equiv \sum_{k=0}^{v-1} q_1^{km} \pmod{v} \\ &\equiv \sum_{k=0}^{v-1} 1 \pmod{v} \\ &\equiv 0 \pmod{v}. \end{aligned}$$

Also for primes $q_2 \equiv 1 \pmod{v}$, we have $\sigma_m(q_2) \bmod v = 2$, since $v \geq 3$. So the hypotheses of Theorem 2 are satisfied, and hence $(\sigma_m(n) \bmod v)_{n\geq 1}$ is not k-automatic. $\square$

Corollary 3 answers the question raised by Allouche and Thakur of whether

$$\sum_{n\geq 1} \sigma_m(n) X^n \in \mathbb{F}_p[[X]] \tag{4}$$

is always transcendental over $\mathbb{F}_p(X)$ for odd primes p [2]. They proved the transcendence of Equation (4) for many cases of p and m in order to give a proof of the function field analogue of Mahler-Manin conjecture. Since $(\sigma_m(n) \bmod p)_{n\geq 1}$ is not p-automatic for primes $p \geq 3$, using Christol's theorem [3] and [4] we get that the formal power series $\sum_{n\geq 1} \sigma_m(n) X^n$ in Equation (4) is always transcendental over $\mathbb{F}_p(X)$.

Corollary 4. *Given $v \geq 3$, the sequence $(\phi(n) \bmod v)_{n\geq 1}$ is not k-automatic for any $k \geq 2$.*

Proof. Note that

$$\phi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}\right) = \prod_{i=1}^{t} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Hence given a prime $q_1 \equiv 1 \pmod{v}$ we have $\phi(q_1) \equiv 0 \pmod{v}$. Also, given a prime $q_2 \equiv -1 \pmod{v}$ we have $\phi(q_2) \equiv -2 \pmod{v}$. Since $v \geq 3$ the hypotheses of Theorem 2 are satisfied. Hence $(\phi(n))_{n\geq 1}$ is not k-automatic. $\square$

Note that $(\phi(n) \bmod 2)_{n\geq 1}$ is k-automatic for all k, since $\phi(n)$ is even for all $n > 2$, and hence $(\phi(n) \bmod 2)_{n\geq 1}$ is constant for $n > 2$.

We also get the following well-known result, which is a direct consequence of the fact that square-free numbers are not k-automatic [5, p. 183].

Corollary 5. *Given an integer $v \geq 2$, the sequence $(\mu(n) \bmod v)_{n\geq 1}$ is not k-automatic for any $k \geq 2$.*

Proof. This is a direct consequence of Theorem 2. □

The proof of Theorem 2 relied heavily on the existence of primes q such that $f(q) \not\equiv 0 \pmod v$. Now we look at another set of multiplicative functions f, where $v|f(q)$ for all primes q, and some integer v. The technique used in this section is different from that used in the proof of the previous theorem, and we need to give the following definition.

Definition 1. Let $T = (t(n))_{n\geq 1}$, and $\#S$ be the number of elements in the set S. Then the *density* of the symbol a in the sequence T is defined to be

$$d(T,a) = \lim_{n\to\infty} \frac{\#\{i \leq n \mid t(i) = a\}}{n},$$

if the limit exists, and is undefined otherwise.

Using this definition we will cite the following lemma due to Minsky and Papert [8], see also [5, p. 184].

Lemma 6. *For any k-automatic sequence F, if $d(F,a) = 0$ then*

$$\limsup_{j\to\infty} \frac{\alpha_{j+1}}{\alpha_j} > 1,$$

where α_j is the position of the j'th occurrence of a.

We now proceed to prove the following theorem.

Theorem 7. *Let $v > 1$ be an integer, and let f be a multiplicative function such that $f(\prod p_i^{\beta_i}) = \prod g(\beta_i)$ for some function g, where the p_i are distinct primes. Also suppose that $g(1) \equiv 0 \pmod v$ and that there exists some integer $h \geq 1$ such that $g(h) \not\equiv 0 \pmod v$. Then $F = (f(n) \bmod v)_{n\geq 1}$ is not k-automatic for any integer $k \geq 2$.*

Proof. First, we need the following lemma.

Lemma 8. *Let f be a multiplicative function such that $f(q) \equiv 0 \pmod v$ for all primes q. Then*

$$d(F,a) = \begin{cases} 1, & \text{if } a = 0; \\ 0, & \text{otherwise.} \end{cases}$$

where $F = (f(n) \bmod v)_{n\geq 1}$.

Proof. Note that if $f(n) \not\equiv 0 \pmod v$, then n is a powerful number (a number where each of its prime factor occurs to a power greater than 1). Choose $a \not\equiv 0 \pmod v$. From [6], see also [7, p. 178], we have that for any $\epsilon > 0$

$$\#\{i \mid i < n;\ i \text{ is a powerful number}\} < n^{\frac{1}{2}+\epsilon},$$

for large enough n. Choosing $\epsilon < \frac{1}{2}$ we get that $d(F,a) = 0$ for $a \neq 0$. Hence the desired result follows. $\square$

Now we are ready to prove our next Theorem. Let $a = g(h) \bmod v$ and α_j be the j'th occurrence of a in F. By definition of h, we get $a \neq 0$. From Lemma 8 we have $d(F,a) = 0$. So if we show that $\limsup_{j\to\infty} \frac{\alpha_{j+1}}{\alpha_j} = 1$, we are done.

On the other hand, note that $(p_i^h)_{i\geq 1}$ is a subsequence of $(\alpha_i)_{i\geq 1}$, where p_i is the i'th prime. Therefore for all j there exists i such that

$$p_i^h \leq \alpha_j < \alpha_{j+1} \leq p_{i+1}^h.$$

Hence

$$1 \leq \frac{\alpha_{j+1}}{\alpha_j} \leq \frac{p_{i+1}^h}{p_i^h}.$$

Therefore

$$\begin{aligned} 1 \leq \limsup_{j\to\infty} \frac{\alpha_{j+1}}{\alpha_j} &\leq \limsup_{i\to\infty} \frac{p_{i+1}^h}{p_i^h} \\ &= \left(\limsup_{i\to\infty} \frac{p_{i+1}}{p_i}\right)^h. \end{aligned}$$

But $\limsup_{i\to\infty} \frac{p_{i+1}}{p_i} = \lim_{i\to\infty} \frac{p_{i+1}}{p_i} = 1$, this is an immediate consequence of the prime number theorem $\lim_{i\to\infty} p_i/i\log i = 1$.

Therefore $\limsup_{j\to\infty} \alpha_{j+1}/\alpha_j = 1$. It follows that F is not k-automatic for any $k \geq 2$. $\square$

Corollary 9. *Given an integer $m \geq 1$, the sequence $(\sigma_m(n) \bmod 2)_{n\geq 1}$ is not k-automatic for any $k \geq 2$.*

Proof. Let $n = 2^\alpha d$, where d is odd. Then we have

$$\begin{aligned} \sigma_m(n) &= \sigma_m(2^\alpha)\sigma_m(d) \\ &= (1 + 2^m + \cdots + 2^{m\alpha})\sigma_m(d) \\ &\equiv \sigma_m(d) \pmod 2 \\ &\equiv \tau(d) \pmod 2. \end{aligned}$$

Furthermore, we know that $\tau(d)$ is odd only when d is a perfect square. So $\sigma_m(n) \bmod 2 = 1$ if and only if n is a perfect square times a power of 2. Let $S = (\sigma_m(n) \bmod 2)_{n\geq 1}$. Then we get $d(S,1) = 0$ since

$$\#\{i \leq n \mid \sigma_m(i) \equiv 1 \pmod 2\} = O(\sqrt{n}).$$

On the other hand if α_n represents the position of the n'th occurrence of 1, we get

$$\begin{aligned} \limsup_{n\to\infty} \frac{\alpha_{n+1}}{\alpha_n} &\leq \limsup_{n\to\infty} \frac{2^\alpha (n+2)^2}{2^\alpha n^2} \\ &= \limsup_{n\to\infty} \frac{(n+2)^2}{n^2} \\ &= 1. \end{aligned}$$

So we have $(\sigma_m(n) \bmod 2)_{n\geq 1}$ is not k-automatic by Theorem 7. □

Also combining Theorems 1 and 2 we get the following new result.

Corollary 10. *For all integers $v, m, k \geq 2$ the sequence $(\tau_m(n) \bmod v)_{n\geq 1}$ is not k-automatic.*

Proof. Assume that for some $v, m, k \geq 2$ the sequence $(\tau_m(n) \bmod v)_{n\geq 1}$ is k-automatic. Therefore by Lemma 1 we get given an integer $p|v$ the sequence $(\tau_m(n) \bmod p)_{n\geq 1}$ is also k-automatic. Therefore assume without loss of generality that v is a prime. Consider the following cases.

Case 1: $m \not\equiv 0 \pmod v$. Then if we choose α and h such that $v^\alpha \parallel m-1$ and $h \equiv 1 - m \pmod{v^{\alpha+1}}$ we get

$$v \quad | \ \tfrac{m+h-1}{m-1}, \Rightarrow v \quad | \ \frac{m+h-1}{m-1}\binom{m+h-2}{m-2} = \binom{m+h-1}{m-1}.$$

Therefore for any prime q we have $\tau_m(q^h) \bmod v = 0$ by (1). On the other hand for all primes q we have $\tau_m(q) \bmod v = m \bmod v \neq 0$. Hence by Theorem 2, we get that $(\tau_m(n) \bmod v)_{n\geq 1}$ is not k-automatic.

Case 2: $m \equiv 0 \pmod v$. Let $g(h) = \binom{m+h-1}{m-1}$. We have that $f(\prod {p_i}^{\alpha_i}) = \prod g(\alpha_i)$ by (1). Also we know $g(1) = m \equiv 0 \pmod v$. Assume that $v^\alpha \parallel m$. Then we get $g(v^\alpha) \not\equiv 0 \pmod v$. Therefore by Theorem 7, $(\tau_m(n) \bmod v)_{n\geq 1}$ is not k-automatic. □

Corollary 10 can be used to prove the transcendence of π_q (an analogue of π in the field $GF(q)((X))$) over the field $GF(q)(X)$ [1].

It is worth mentioning that both of our theorems relied on $v|f(n)$, for some n. If f is multiplicative and $v \nmid f(n)$ for any $n \geq 1$, then its the analysis becomes much more difficult. For example the Liouville function defined by

$$\lambda(p_1^{\alpha_1} \cdots p_t^{\alpha_t}) = (-1)^{\alpha_1+\cdots+\alpha_t},$$

is never divisible by any prime. It seems that the question of whether or not $(\lambda(n))_{n\geq 1}$ is k-automatic is an open problem worth pursuing.

Acknowledgement. I would like to thank J. Shallit for simplifying the proof of Theorem 2, and suggesting different generalizations of the original problem, and many other helpful suggestions. Also I would like to thank the referee for many valuable suggestions, and P. Borwein, G. Almkvist, and W. L. Yee for all their help in the preparation of the original draft.

References

[1] J.-P. Allouche, *Sur la transcendance de la série formelle* π. Sém. Théor. Nombres Bordeaux **2** (1990), 103–117.

[2] J.-P. Allouche, D. S. Thakur, *Automata and transcendence of the Tate period in finite characteristic.* Proc. Amer. Math. Soc. **127** (1999), 1309–1312.

[3] G. Christol, *Ensembles presque périodiques k-reconnaissables.* Theoret. Comput. Sci. **9** (1979), 141–145.

[4] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, *Suites algébriques, automates et substitutions.* Bull. Soc. Math. France **108** (1980), 401–419.

[5] A. Cobham, *Uniform tag sequences.* Math. Systems Theory **6** (1972), 164–192.

[6] P. Erdös, G. Szekeres, *Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem.* Acta Sci. Math. (Szeged) **7** (1935), 95–102.

[7] A. Ivić, P. Shiu, *The distribution of powerful integers.* Illinois J. Math. **26** (1982), 576–590.

[8] M. Minsky, S. Papert, *Unrecognizable sets of numbers.* J. Assoc. Comput. Mach. **13** (1966), 281–286.

[9] R. Sivaramakrishnan, *Classical theory of arithmetic functions.* Monographs and Textbooks in Pure and Applied Mathematics **126**, Marcel Dekker, Inc., New York, 1989.

Soroosh Yazdani
Department of Mathematics
University of Illinois
273 Altgelt Hall, MC-382
1409 W. Green Street
Urbana, IL 61801
USA
E-mail : syazdani@math.uiuc.edu